

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

I, Patrick Grady, being duly sworn, state the following:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I am a Detective with the Natick Police Department and have been assigned as a Task Force Officer (“TFO”) with the Drug Enforcement Administration (“DEA”) since April 2022. I am currently assigned to the Organized Crime Drug Enforcement Task Force (“OCDETF”) Strike Force located in Waltham, Massachusetts, which is a task force incorporating various law enforcement agencies, including DEA, the Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”), the Federal Bureau of Investigation (“FBI”), Immigrations and Customs Enforcement Homeland Security (“HSI”), and the U.S. Marshals Service (“USMS”) among other state and local agencies. I am a graduate of the Boston Police Academy and have been a police officer since 2015. During my time as an officer and TFO, I have investigated a variety of criminal offenses, including state and federal drug offenses.

2. As a police officer and DEA TFO, I am authorized to investigate violations of the laws of the United States, including violations of federal narcotics laws in Title 21 of the United States Code. I have received training regarding narcotics investigations while attending the Boston Police Academy and have attended additional specialized training courses in furtherance of my past and current assignments.

3. I have written and/or participated in the execution of numerous search warrants resulting in the seizure of large quantities of controlled substances and paraphernalia involved in

the manufacture and distribution of controlled substances, United States currency, records of narcotics and monetary transactions, drug customer lists and other documents relating to the manufacturing, transportation, ordering, purchasing and distribution of controlled substances, as well as the collection, expenditure, accounting, transportation, and laundering of drug proceeds. I have participated in the debriefing of numerous defendants, informants, and witnesses who had personal knowledge regarding large-scale narcotics trafficking organizations. I have participated in all aspects of drug investigations including conducting surveillance, executing searches pursuant to court-ordered search warrants, executing arrests, and participating in court-authorized wiretap investigations.

#### **PURPOSE OF AFFIDAVIT**

4. This affidavit is being submitted in support of an application for a warrant to search electronic equipment, specifically a black Apple iPhone that was seized on November 17, 2019, from 7 Morse Street, Apartment #1 in Natick, Massachusetts, the residence of Rafael ASHWORTH (the “Subject Phone”). The Subject Phone, which is described in Attachment A, has been in the possession of law enforcement investigators since the time of its seizure.

5. On February 10, 2021, a Boston federal grand jury returned an indictment charging ASHWORTH with possession with intent to distribute fentanyl, methamphetamine, and heroin, in violation of 21 U.S.C. § 841, and distribution of and possession with intent to distribute fentanyl resulting in death, in violation of 21 U.S.C. § 841(a)(1) and (b)(1)(C) [Case No. 19-cr-10477-WGY<sup>1</sup>]. The case is set for trial on January 29, 2024. As set forth herein, there is probable cause to believe that the Subject Phone contains evidence, fruits, and instrumentalities of the charged

---

<sup>1</sup> The case was originally assigned to a different judge but was reassigned in December 2023 to the Honorable William G. Young.

crimes, as described in Attachment B.

6. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

#### **PROBABLE CAUSE**

7. On November 17, 2019, ASHWORTH was arrested at his residence, 7 Morse Street, Apartment #1 in Natick, Massachusetts, after officers from the Natick Police Department responded to the location to investigate a reported overdose. When officers arrived, they encountered ASHWORTH, who appeared to be intoxicated. In the sole bedroom inside the apartment, officers discovered the body of a deceased woman lying in the bed. On the side of the bed, officers observed in plain sight a pill press and what appeared to be controlled substances. Officers removed ASHWORTH from the scene, secured the apartment, obtained a search warrant, and later returned to search the apartment.

8. During the search, officers recovered three iPhones and an iPad from ASHWORTH's bedroom along with other items evidencing drug trafficking, including the pill press, a bag containing 99 grams of a mixture of fentanyl, methamphetamine, and heroin, kilograms of powder used to dilute drugs and manufacture counterfeit narcotic pills, sifters, digital scales, and a mixing bowl. On December 10, 2019, officers obtained a federal search warrant to search one of the three iPhones seized from the bedroom, which was believed to be ASHWORTH's phone [Dkt. No. 19-mj-1448-DLC]. The affidavit submitted in support of that search warrant is attached hereto as Exhibit 1 and incorporated herein. Extractions later determined that searched phone was in fact ASHWORTH's phone (hereinafter, referred to as the "ASHWORTH Phone"),

and evidence of the charged crimes was recovered from the ASHWORTH Phone. That evidence included videos of ASHWORTH pressing counterfeit narcotic pills using the pill press recovered from his apartment and numerous text messages with drug customers and suppliers in which ASHWORTH discussed the manufacture, packaging, delivery, prices, and sale of narcotics.

9. The parents of the deceased identified the iPad and a white iPhone 7 with a pink back that was seized from the bedroom (hereinafter, the “white iPhone”) as belonging to the deceased. Both of these devices were powered off when they were recovered. With the consent of the deceased’s parents, investigators attempted to examine the contents of the white iPhone and iPad but could not unlock them because they did not have the passcodes to either. Investigators accompanied the deceased’s father to an Apple store to seek their assistance, but Apple could not provide any assistance. The iPad and white iPhone were sent to a law enforcement laboratory for forensic examination. The extraction equipment used by the laboratory in 2019/2020 was not sophisticated enough to unlock or extract any data from the iPad or white iPhone.

10. In December 2019, investigators did not seek a warrant to search the Subject Phone when they obtained the warrant to search the ASHWORTH Phone because the technology used by law enforcement at that time could not unlock newer versions of iPhones, including an iPhone 11.

11. In December 2023, the government resubmitted the white iPhone for forensic evaluation. The updated technology used by law enforcement was able to extract data from the white iPhone. The extractions revealed that the white iPhone believed to have belonged to the deceased in fact was not the deceased’s phone. For example, the phone number associated with the white iPhone was not the deceased’s phone number. Additionally, there were no indicia of the deceased’s ownership contained in the data extracted from the white iPhone.

12. Based on the recent success in extracting data from the white iPhone and my discussions with forensic technicians, investigators now believe that the updated technology might allow them to extract data from the Subject Phone, including the phone number. Based on the fact that the Subject Phone was seized from ASHWORTH's bedroom at the time of his arrest and evidence of the charged crimes was found on the ASHWORTH Phone, there is probable cause to believe additional evidence of the charged crimes may be found on the Subject Phone.

#### **Investigators' Possession of the Subject Phone**

13. As stated above, the Subject Phone has been in the possession of the government since November 17, 2019, and has been stored in a manner which prevented it from being altered. Since the date of the seizure, neither the defendant nor his counsel has not requested that the Subject Phone be returned or viewed.<sup>2</sup>

#### **Drug Traffickers' Use of Cell Phones Generally**

14. Based on training and experience, I know that most drug dealers regularly use cellular telephones to communicate about their drug trafficking activities with customers, suppliers, and other coconspirators. In my training and experience, I also am aware that drug traffickers are often aware of law enforcement's use of electronic surveillance, and thus frequently change cellular telephone numbers and/or use multiple cellular phones at the same time, as well as prepaid cellular phones (where the subscriber of the phone is not required to provide personal identifying information), in an effort to thwart law enforcement's use of electronic surveillance. Because cellular telephones are often a principal means of communication, drug dealers typically keep the phones in close proximity or at their residences.

---

<sup>2</sup> Moreover, even if the defendant had requested the phone's return, he has been incarcerated since November 17, 2019, and would not have been permitted to possess the phone in his detention facility.

15. Based upon my knowledge, training, and experience, I know that a cellular telephone is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through networks of transmitter/receivers called “cells,” enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones now offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include GPS technology for determining the location of the device. Based on my training and experience, I know that many cellular telephones have the capabilities described above.

16. Search of devices containing this information will provide information relating to coconspirators and accomplices. I know, based upon my training and experience, as well as consultation with other investigators, that individuals who sell illegal drugs typically use cellular telephones to communicate with their suppliers, their customers, and with other coconspirators, and that they communicate both via voice calls and via email and/or text messaging. I also know that persons who sell illegal drugs regularly keep records of their illegal activities. These records can include, but are not limited to, contact list of buyers and sellers, ledgers of sales and money owed by customers or to suppliers, and lists of quantities and/or specific controlled substances preferred by or ordered by specific customers. Individuals engaged in drug trafficking activities

often take photographs of their closest confederates. Records of drug trafficking activities can be produced and maintained on paper in a tangible form and/or by electronic means on a cellular telephone. From my training and experience, and information provided to me by other agents, I am aware that individuals commonly store records of the type described in Attachment B on their cellular telephones.

17. Additionally, I know that many drug traffickers often use cellular telephones in order to communicate quickly and economically with their suppliers and customers via the internet. I am also aware that individuals frequently use cellular telephones to create and store records of their actions by communicating with others through e-mail, electronic messages, and updates to online social-networking websites; keeping their calendars; arranging for travel; storing pictures; researching topics related to drug trafficking; and accessing their bank, financial, investment, utility, and other accounts online. Additionally, many cellular phones today have a GPS navigation device on the phone. Examination of the GPS data on a cellular phone can provide valuable evidence as to the locations where drug traffickers meet with coconspirators, including their sources of supply, and can aid in identifying those individuals. Additionally, review of GPS data can aid in identifying offsite locations where drug traffickers store drugs, maintain bank accounts, and conceal their drug proceeds.

18. Based upon my training and experience, and information provided to me by others involved in the forensic examination of computers, I know that electronic data on cellular telephones can be stored in a variety of methods, including, but not limited to, within the memory of the cellular telephone; within volatile memory, such as RAM; or on removable media, such as memory cards. I also know that electronic data can often be recovered months or even years after it has been written, downloaded, saved, deleted, or viewed locally or over the internet. This is true

because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their electronic equipment, they can easily transfer the data from their old device to a new one.
- b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a device, the data contained in the file often does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, the device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, electronic storage media often contains electronic evidence of how the device has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but users typically do not erase or delete this evidence because special software is typically required for that task.
- d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser on a cellular telephone often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

19. Based on the forgoing, including the drugs seized from ASHWORTH’s residence and the evidence of drug trafficking that was extracted from the ASHWORTH Phone, I have probable cause to believe that the Subject Phone contains evidence, fruits, and instrumentalities of the crimes charged in the Superseding Indictment.



Sworn to under the pains and penalties of perjury,

Patrick Grady DLC  
Patrick Grady  
DEA Task Force Officer

Subscribed to and sworn before me telephonically in accordance with the requirements of Fed. R. Crim. P. 4.1 on January 19, 2024.

[Signature]  
Honorable Donald L. Cabell  
Chief United States Magistrate Judge



## **ATTACHMENT A**

### **Description of Equipment to Be Searched**

The Subject Phone to be searched is a black iPhone seized on November 17, 2019, from 7 Morse Street, Apartment #1 in Natick, Massachusetts, the residence of Rafael ASHWORTH. The Subject Phone is in the custody of the government. Below are photos of the Subject Phone to be searched.



## **ATTACHMENT B**

### **Items to Be Seized**

I. All records, from August 2019 through November 2019, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 21 U.S.C. § 841(a)(1) (distribution of and possession with intent to distribute fentanyl, methamphetamine, and heroin), and 21 U.S.C. § 841(a)(1) and (b)(1)(C) (distribution of and possession with intent to distribute fentanyl resulting in death) including those related to:

1. All names, words, telephone numbers, email addresses, time/date information, messages or other electronic data relating to or referencing drug trafficking and/or referencing individuals engaged in drug trafficking located in the equipment of the Subject Phone, including but not limited to:
  - a. Names and contact information that have been programmed into the device (including but not limited to contacts lists) of individuals who may be engaged in drug trafficking;
  - b. Logs of calls (including last numbers dialed, last calls received, time of calls, missed calls, and duration of calls) both to and from the device;
  - c. Text messages both sent to and received by the device (including any in draft form) relating to or referencing drug trafficking and/or referencing individuals engaged in drug trafficking;
  - d. Incoming and outgoing voice mail messages both to and from the device relating to or referencing drug trafficking or individuals engaged in drug trafficking;
  - e. GPS data;

- f. Browser messages and/or internet communications (e.g., e-mail, text messages) both to and from the device (including any in draft form) relating to or referencing drug trafficking or individuals engaged in drug trafficking;
  - g. Documents, photographs, or videos in any format, including but not limited to Microsoft Word or Adobe PDF files, relating to or referencing drug trafficking or individuals engaged in drug trafficking;
  - h. All data within the device evidencing ownership, possession, custody, control, or use of the device; and
  - i. Service Provider handset unlock password(s) and any other passwords used to access the electronic data described above.
2. Serial numbers and any electronic identifiers that serve to identify the computer equipment.

### **DEFINITIONS**

For the purpose of this warrant:

- B. “Equipment” means any hardware, software, storage media, and data.
- C. “Hardware” means any electronic device capable of data processing (such as a computer, digital camera, cellular telephone or smartphone, wireless communication device, or GPS navigation device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

- D. “Software” means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.
- E. “Storage media” means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or thumb drive, or memory card).
- F. “Data” means all information stored on storage media of any form in any storage format and for any purpose.
- G. “A record” is any communication, representation, information or data. A “record” may be comprised of letters, numbers, pictures, sounds or symbols.

### **Return of Seized Equipment**

If, after inspecting seized equipment, the government determines that the equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy’s authenticity and accuracy (but not necessarily relevance or admissibility) for evidentiary purposes.

If equipment cannot be returned, agents will make available to the equipment’s owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, personally-identifying information of victims; or the fruits or instrumentalities of crime.